The coherence function (Fig. 3) as a function of frequency was calculated between the synchronised undistorted and distorted signals. The SNR (f) was obtained from the coherence function (Fig. 4*b*), and this was compared with the 'real' SNR (f) obtained from the signal and noise spectra (Fig. 4*a*), showing almost similar results.

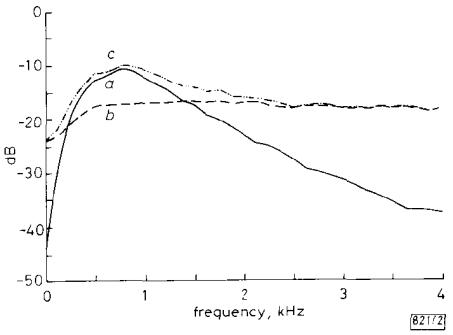

Fig. 2 *Power spectral density of (a) undistorted test signal, (b) white noise and (c) distorted test signal*

The following FFT parameters were used to calculate the auto- and cross-Welch periodograms:

Total block size	4096 samples
FFT frame size	64 samples
Frame overlap	50%
Number of averages	127
Window type	Hamming

Conclusion: The above results indicate the possibility of using the coherence function as means of SNR (f) measurements at the output of communication systems when a speech-simulating test signal is used. The method requires a clean reference copy of the transmitted test signal at the output of the system which has to be synchronised with the distorted output of the channel.

The periodogram parameters determine the accuracy of SNR (f), which depends on the bias and variance errors of $G_x(f)$, $G_{yy}(f)$ and $G_{xy}(f)$, where there is a trade-off between the levels of errors and the desired frequency and time resolution.[5] Increasing the frequency resolution leads to a reduction in the bias errors but an increase in the variance. It is, however, possible to reduce the variance errors in SNR (f), having achieved acceptable bias errors, by smoothing the data points using a simple digital filter.

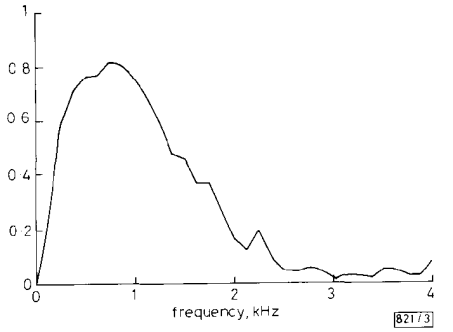

Fig. 3 *Coherence function between undistored and distorted test signals*

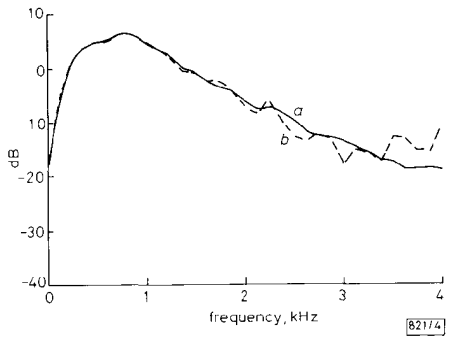

Fig. 4 *SNR (f) calculated from (a) signal and noise spectra and (b) coherence function*

I. JALALY

Electronic Engineering Laboratories
University of Kent
Canterbury, Kent CT2 7NT, United Kingdom

1st September 1989

References

1 CCITT Recommendation G.22-1, Geneva, 1968
2 BENDAT, J. S., and PIERSOL, A. G.: 'Random data analysis and measurement procedure' (Wiley-Interscience, J. Wiley & Sons, 1986)
3 ROTH, P. R.: 'Effective measurements using digital signal analysis', *IEEE Spectrum*, April 1971, pp. 62–70
4 WELCH, P. D.: 'The use of fast Fourier transform for the estimation of power spectra: a method based on time averaging over short, modified periodograms', *IEEE Trans.*, 1967, **AU-15**, pp. 70–73
5 BENDAT, J. S.: 'Statistical errors in measurement of coherence functions and input/output quantities', *J. Sound & Vib.*, 1978, **59**, pp. 405–421

METHOD TO IMPLEMENT PACKET LEVEL ACCESS CONTROL IN MULTINETWORKS

Indexing terms: Networks, Telecommunications, Information theory, Data transmission

The letter describes a method to implement an access control policy for multinetwork environments. The access control method is based on the public-key cryptosystem proposed by Rivest, Shamir and Adleman (RSA) and on the message authentication algorithm based on Data Encryption Standard (DES).

Method description: This scheme implements a nondiscretionary access control policy. A similar scheme, called the Visa scheme,[1] requires key distribution for each external data transfer request. Here a complete practically realisable system not requiring key distribution for authenticating each external packet is presented. The general model for which the proposed method will work is shown in Fig. 1. The entities participating in the global access control policy are the host machines and the access control gateways. Access control gateways are assumed to be highly secure and trusted machines. The overall method is explained by an example.

Consider that HostA in Network1 wants to access HostC in Network3 (Fig. 1). HostA knows that it is an external access request. It will send a request packet indicating the destination network and the destination host address to the Network12 access control gateway (N12ACG). N12ACG knows the following facts:

(1) if the registered hosts are allowed to access external networks, and their capabilities (capability defines the external resources and the external networks to which the hosts are allowed access);

(2) the externally accessible resources of each external network, reachable through it.

If the intersection of the HostA access list and Network3 access list is nonempty, authorisation success is reported in N12ACG. After verifying the host's accessibility and the capability rights, N12ACG authenticates hostA. Failure of the access capability rights or authentication failure at any access

control gateway will result in refusal of the external access request. Communication between two entities can only take place once a secure communication path has been set up.

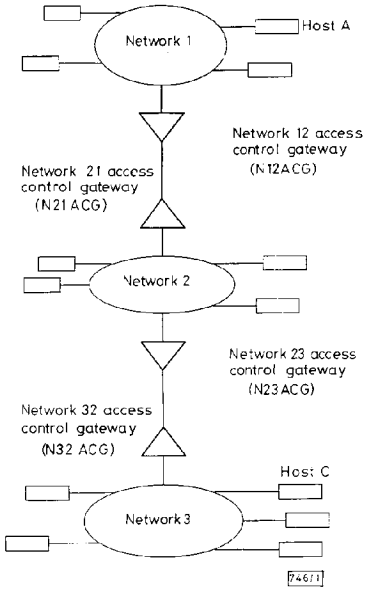

Fig. 1 *General model of multinetwork environment*
General model extendable to *N* interconnected networks

The authentication protocol uses the RSA public key algorithm.[2] The protocol works as follows. N12ACG randomly selects a session initiation authenticator (an integer identifier less than the modulus of an RSA system), encrypting it using the public key of HostA, and sending it to HostA. Then HostA recovers the authenticator using its private key, and sends the authenticator in clear back to the N12ACG. This protocol ensures that only the host machine possessing the correct private key can decode the session initiation authenticator. On receiving the correct authenticator from HostA, N12ACG enters into a dialogue with access control gateway of Network2. N12ACG first sends a request containing the destination network and the destination host address to Network21 access control gateway (N21ACG). N21ACG has the access list and the capability list for Network1. (Here the capability defines the networks to which Network1 is allowed access.) N21ACG applies intersect rule, and on nonempty intersection, authorisation success is reported. On initial clearance N21ACG authenticates N12ACG according to the above explained authentication protocol. (Obviously, they share a different RSA public private key pair.) Having authenticated the N12ACG, N23ACG enters into an identical dialogue on the behalf of Network1 with Network32 access control gateway (N32ACG). N32ACG checks if Network1 is allowed to access HostC. On nonempty intersection between the requested resource and the allowable resource list of Network1, N32ACG checks if the requested HostC is up and ready, and if so then N32ACG sends an access allowed packet to N23ACG. Included in the access allowed packet is a reference number indicating the cryptographic key to be used by N23ACG while computing the packet authentication code.

The reference number is an integer specifying an offset to the RSA private key of each participant. From this offset the next 56 bits form the packet authentication key (PAK) to be used for calculating the packet authenticating code. Each access control gateway keeps a list, mapping the PAK with the source destination identity of the requesting machine. This mapping is only valid for the current source destination session. A new reference number is issued for each subsequent request. At any time there could be a long list of PAKs to source destination mapping.

The packet authentication code (PAC) is used to verify the data originality of each packet after external access is allowed. The packet authentication code ensures that only the holder of the packet authentication key is allowed to transport external packets. N21ACG chains the access permission to N12ACG. N21ACG also indicates through a reference number the packet authentication key to be used by the N12ACG while exporting packets from HostA to HostC on Network3. Network2 acts here as a transit traffic handler. Depending on the global access policy, Network 2 access control gateway may or may not enforce control policy on the traffic not intended for Network2 hosts. It would be in this case transparent for Network1 and Network3. N12ACG completes the external access request procedure by sending an external access request success packet to HostA. Included in the packet is the reference number to be used by HostA for authenticating each external packet during the period of external access.

HostA, having received the reference number from the N12ACG, goes into packet control mode. The other entities participating in the external transfer session have already received the reference number, and are in the packet control mode. Here it is assumed that each entity participating in the access control mechanism is running the connectionless network service protocol ISO 8473.[3] The packet level authenticator can be placed in the protocol by utilising the options field of the protocol. The options field is provided for indicating the security functions implemented in the network layer.

The DES[4] private key algorithm is used to calculate the packet authentication code. Using the reference number 56 bits are computed from the RSA private key. These 56 bits form the DES key. Hence, there is no need to distribute DES keys. Each entity participating in the session derives the DES key from it's own RSA private key.

HostA computes the packet authentication code (PAC) using the key derived from the RSA private key. This PAC is then appended in the options field of the ISO 8473 protocol, and sent to Network1 access control gateway. A parameter code byte in the options field indicates the presence of packet authenticator. The complete protocol data structure received at Network1 access control gateway is shown in Fig. 2.

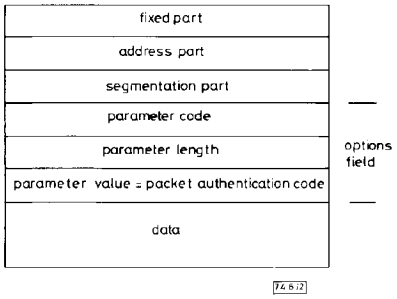

Fig. 2 *ISO 8473 protocol data unit structure including options field*

Network1 access control gateway, on receiving the packet, authenticates the packet by recomputing the PAC using the same PAC key as used by HostA. On verification it recomputes the PAC, this time using the agreed PAC key with the Network2 access control gateway. Network2 access control gateway, after verification, recomputes the PAC using agreed key with the Network3 access control gateway. Network3 access control gateway, on authentication success, sends the packet to HostC. This pattern for packet transportation is followed until the whole message has been transported from HostA to HostC.

Salient features of scheme: Each time an external access is requested, a new reference number is issued by the access control gateway to the requesting host. This results in a new

PAC key for each external request. Only packets including PAC based on this new key are transported to the next access gateway in the hierarchy of interconnected networks. This ensures the uniqueness of the PAC key for each external session. Hence, no PAC key is valid for more than one authorised session. The PAC keys are automatically nulled at the closure of the connection. The RSA private key is normally 664 bits long. This allows a wide range of PAC keys. The keys are selected by specifying an integer offset from the start of the RSA key pattern, or from the end counting backward. The direction of key selection is indicated by a bit value sent with the reference number on the success of session initiation authentication. A new RSA key can be sent to the hosts by their respective access control gateways. This new key can be sent using the old public key of the host. If the old private key has been compromised then manual installation of the key should take place. A new RSA key allows a whole range of new PAC keys. The scheme described allows different networks to formulate their own internal access control services and mechanisms to implement these services. Similarly, the access control protocol between the access control gateways could also be varied. The method would work independently of any application running on top of the network layer.

Conclusion: A hierarchical approach to implement packet level access control in multinetworks has been described. The described approach does not require distribution of PAC keys. Moreover, a network only needs a common access control policy with its communication access control gateways. Each network can have an independent internal access policy, and separate mechanisms to implement this policy.

F. S. F. POON
S. M. IQBAL

School of Engineering & Applied Sciences
University of Sussex
Falmer, Brighton BN1 9QT, United Kingdom

21st August 1989

References

1 ESTRIN, D.: 'Interconnection protocols for interorganisation networks', *IEEE J. Sel. Areas Commun.*, Dec. 1987, **SAC-5**, (9)
2 RIVEST, R. L., SHAMIR, A., and ADLEMAN, L.: 'A method for obtaining digital signatures and public key cryptosystems', *Commun. ACM*, Feb. 1978, **21**, (2)
3 'Information processing systems—data communications—protocol for providing the connectionless-mode network service'. International Organisation for Standardisation, ISO 8473, 1988
4 ZIMMERMAN, P.: 'A proposed standard format for RSA cryptosystems', *IEEE Computer*, Sept. 1986

NEW APPROACH TO ANALYSIS OF QUANTUM RECTIFIER-INVERTER

Indexing terms: Power supply circuits, Control theory, Inverters, Convertors

The quantum rectifier-inverter, a new class of cycloconvertor, is analysed by a new analysis based on quantum transformation. The switching pattern of the quantum convertor is determined by a very simple logic circuit. It is verified that the operation of the quantum convertor is the same as that of the conventional rectifier-inverter.

Introduction: A new class of quantum convertors, which are a kind of resonant convertor with nearly zero switching losses, has been proposed in recent papers on higher switching frequency operation.[1-3] Since their switching frequency should be fixed to the circuit resonance frequency, control of them is by quantised time-domain selection of discrete pulses. The name 'quantum' stems from the quantised time-domain control and quantised output levels. This quantisation feature makes it difficult to deal with the new convertors. Until now none of the systematic control schemes and analysis techniques for the quantum rectifier-inverters have been available.

It has been verified that quantum DC/DC convertors are equivalent to conventional PWM DC/DC convertors.[2] It is natural to also expect conventional convertors to be equivalent to quantum rectifier-inverters. Therefore a new way to analyse quantum convertors, 'quantum transformation', is proposed in this letter.

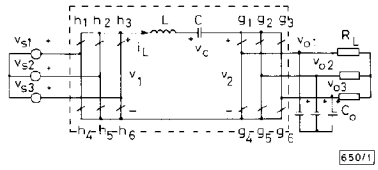

Fig. 1 *Quantum rectifier-inverter*

Quantum transformation: The system to be modelled is composed of ideal switches as shown in Fig. 1. The resonant tank current i_L is regulated by the rectifier and is fed to output AC capacitor by the inverter to form the wanted output voltage. The aim of this letter is to find the appropriate switching pattern for control, and DC voltage gain expression of this system. The key problem is to simplify the resonant circuit.

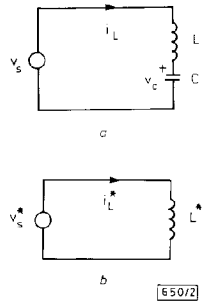

Fig. 2 *Series resonant LC tank*
a Original circuit *b* Equivalent circuit

Consider first the resonant circuit and the waveforms as shown in Figs. 2 and 3, respectively. In Fig. 3 the v_s^*, i_L^* are defined to be the products of $q(t)$ and v_s, i_L, respectively. Noting the fact that the envelope of i_L is linear, it is not difficult to recognise that the relationship between Figs. 3*d* and *f* is much more illustrative than that between Figs. 3*a* and *b*.

Then the inductor current of Fig. 2*a* is found to be as follows:[1]

$$i_L = \left[I_p(k-1) + 2S\left(\frac{C}{L}\right)^{1/2} V_s \right] q(t) \sin \omega\left(t - \frac{kT}{2}\right) \quad \text{for } \frac{kT}{2} < t < \frac{k+1}{2} T$$

$$S = 1 \text{ for } A \qquad S = 0 \text{ for } B \qquad S = -1 \text{ for } C \quad (1a)$$

where

$$I_p(k) = \text{peak of } [i_L q(t)]$$

$$q(t) = -1 + 2u(t) - 2u\left(t - \frac{T}{2}\right) + 2u(t - T) - \ldots \quad (1b)$$

and $u(t)$ is a unit step function. Now the quantum transformation is defined for an arbitrary variable $x(t)$ as

$$x^*(t) \equiv q(t)x(t) = q(t)\frac{2}{T}\int_{kT/2}^{(k+1)/2)T} x(t)\,dt \quad \text{for } \frac{kT}{2} < t < \frac{k+1}{2} T \quad (2)$$